REMARKS

Claims 1-9 are pending in the current application. In an Office Action dated March 28, 2005 ("Office Action"), the Examiner objected to claims 1 and 2, rejected claim 1 under 35 U.S.C. § 102(b) as being anticipated by Eastlake et al., "Randomness Recommendations for Security," RFC 1750, December 1994, pp. 1-30 ("Eastlake"), rejected claim 2 under 35 U.S.C. § 103(a) as being unpatentable over Eastlake in view of Ritter, "The Hardware Random Number Generator: A Ciphers by Ritter Page," pp. 1-145 ("Ritter"), rejected claim 3 under 35 U.S.C. § 103(a) as being unpatentable over Eastlake in view of Ritter and further in view of "Individual Logic Gates and De Morgan's Theorem," pp 1-10 ("Logic Gates"), rejected claim 4 under 35 U.S.C. § 103(a) as being unpatentable over Eastlake in view of Saito, U.S. Patent No. 6,542,014 B1 ("Saito"), rejected claim 5 under 35 U.S.C. § 103(a) as being unpatentable over Eastlake in view of Dultz et al., U.S. Patent No. 6,609,139 B1 ("Dultz"), rejected claim 6 under 35 U.S.C. § 103(a) as being unpatentable over Eastlake in view of Vincze et al., U.S. Patent No. 6,369,727 B1 ("Vincze"), rejected claim 7 under 35 U.S.C. § 103(a) as being unpatentable over Eastlake in view of Larson et al., U.S. Patent No. 4,641,840 ("Larsen"), rejected claim 8 under 35 U.S.C. § 103(a) as being unpatentable over Eastlake in view of Buhler et al., EP 1 081 591 A2 ("Buhler"), and rejected claim 9 under 35 U.S.C. § 103(a) as being unpatentable over Eastlake in view of Chan et al., U.S. Patent No. 6,046,616 ("Chan"). Applicants' representative has cancelled claims 1-9, in the above amendment, and has added new claims 10-13 to more distinctly and particularly claim that which Applicants regard as their invention. Although claims 1-9 are cancelled, Applicants' representative nonetheless traverses certain of the above-listed rejections that might be modified and re-applied to newly added claims 10-13.

Applicants' representative first acknowledges that the Examiner has provided pertinent cited references for a number of the above-listed rejections. It is a pleasure to respond to a well considered and well-researched Office Action. However, in several rejection, Applicants' representative believes that the cited references are not relevant, and do not address the claim language against which they were cited.

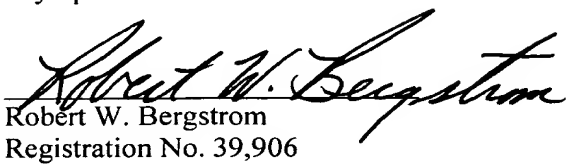
As a first example, the citation of Logic Gates and Eastlake in the

rejection of claim 3, is seemingly not relevant to the merging component (13 in Figure 1) of the claimed invention. The claimed merging component "merges the compressed data streams output by the compressors to produce a merged, compressed data stream that is output to the monitor and random number generator." The trivial mixing function disclosed in Eastlake is directed to "converting a stream of bits that is skewed towards 0 or 1 to a shorter stream which is more random" (Eastlake, section 6.1, page 12) and not to merging two or more different compressed data streams. Logic Gates is a simple primer on TTL logic gates, and neither discloses nor suggests random number generation, compressed data streams, or merging of compressed data streams. The combination of Eastlake and Logic Gates does not teach, mention, or suggest merging compressed data streams, as clearly claimed in newly added claim 11, within a random number generation device.

As a second example, the citation of Chan and Eastlake in the rejection of claim 9, is seemingly not relevant to the blocking switch (17 in Figure 1) of the claimed invention. Chan's HOLD signal "prevents the generation of one pseudo random binary number during a clock cycle" within a pseudo random pulse generator (Chan, Abstract and lines 12-14 of column 3). Chan's HOLD signal is part of a timing mechanism used to synchronize random number generation within a clock-controlled circuit. Chan neither teaches, mentions, nor suggests blocking random number generation until sufficient data has been received from a compressed data stream, or from any other source, to generate a random number. Chan's HOLD signal fires periodically, at a similar point in each clock cycle, and is released periodically at another point in the clock cycle, to synchronize random number output with the clock cycles. Since the HOLD signal is asserted periodically, it is clearly not asserted based on any kind of decision regarding sufficient accumulation of data. Moreover, Chan does not mention of suggest generation of random numbers from a compressed data stream. Claim 1, by contrast, includes the language: "a blocking switch controlled by the monitor to block output of a next random number by the random number generator when sufficient data to generate the next random number has not been received in the compressed data stream to generate a next random number."

In Applicants' representative's opinion, all of the claims remaining in the application are now clearly allowable. Favorable consideration and a Notice of Allowance are earnestly solicited.

Respectfully submitted,
Gadiel Seroussi et al.
Olympic Patent Works PLLC



Robert W. Bergstrom
Registration No. 39,906

Enclosures:
Postcards (2)
Transmittal in duplicate

Olympic Patent Works PLLC
P.O. Box 4277
Seattle, WA 98194-0277
206.621.1933 telephone
206.621.5302 fax